WHAT IS CLAIMED

1. A node of a network maintaining an instance of an intrusion prevention system, the node comprising:

a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver and bound to the protocol driver and the media access control driver, the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive at least one of a plurality of machine-readable network-exploit signatures from a database and provide the at least one machine-readable network-exploit signatures to the associative process engine, the associative process engine operable to compare a packet with the at least one machine-readable network-exploit signature and determine a correspondence between the packet and the at least one machine-readable network-exploit signature.

2. The node according to claim 1, wherein the database is maintained in a storage device of the node.

3. The node according to claim 1, wherein each of the plurality of machine-readable network-exploit signatures comprise a respective directive that defines instructions to be executed upon determination of a correspondence between the packet and the respective exploit signature.

4. The node according to claim 1, wherein, upon determination of a correspondence between the packet and two or more of the plurality of machine-readable network-exploit signatures, each of the directives of the two or more machine-readable network-exploit signatures are executed by the intrusion prevention system.

5. The node according to claim 1, wherein, upon determination of a correspondence between the packet and two or more of the plurality of machine-readable network-exploit signatures, an alternative directive is executed, the alternative directive dependent upon the combination of the two or more network-exploits signatures having a correspondence with the packet.

6. A method of analyzing a packet at a node of a network by an intrusion prevention system executed by the node, comprising:

reading the packet by the intrusion prevention system;

comparing the packet with a plurality of machine-readable network-exploit signatures; and

determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures.

7 The method according to claim 6, further comprising generating a record of the at least two of the plurality of machine-readable network-exploit signatures with which a correspondence with the packet is made.

8. The method according to claim 7, further comprising transmitting the record to a management node connected to the network.

9. The method according to claim 7, further comprising logging the record in a database.

10. The method according to claim 6, further comprising executing, by the intrusion protection system, a respective directive of each of the at least two machine-readable signatures determined to correspond with the packet.

11. The method according to claim 6, further comprising executing, by the intrusion protection system, at least one directive of at least one of the machine-

readable network-exploit signatures of the record determined to have a correspondence with the packet.

12. The method according to claim 6, further comprising executing, by the intrusion protection system, an alternative directive dependent on the record of machine-readable signatures determined to have a correspondence with the packet.

13. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

comparing a packet with a plurality of machine-readable network-exploit signatures;

determining a correspondence between the packet and at least a subset of the plurality of machine-readable network-exploit signatures; and

generating a record of the subset with which the correspondence is made.

14. The computer readable medium according to claim 13, further comprising a set of instructions that cause, when executed by the processor, the processor to perform a computer method of:

determining a correspondence between the packet and a subset of the plurality of machine-readable network-exploit signatures, each machine-readable network-exploit signature comprising a directive; and

executing, by the processor, each directive of the record of machine-readable signatures.

15. The computer readable medium according to claim 13, further comprising a set of instructions that cause, when executed by the processor, the processor to perform a computer method of

executing a directive dependent on the machine-readable network-exploit signatures within the subset.